WSATA Conference - 2013

○ Staff Consolidation – 2006

   ○ Developers, Desk Top Support, Security, DBA

○ Server Consolidation – 2009

○ Security of Data Systems

○ Google Security

Data Center Consolidation Initiative

- The project was successfully completed in a short 12 months, with a 6 month planning period beforehand.

- The results of the project include:
  - Reduced the number of data centers in the State from 35 to 2
  - Reduced the total number of physical servers from 1864 to 591
  - Save the State $4 million annually ongoing in server, support, and energy costs
  - Increased security
  - Increased performance

Consolidation January 6, 2009

- **Communication essential between Agency and Enterprise (State Data Center)**
  - Timing is a critical factor to the agency
  - Data ownership - by the Agency
  - Applications & Data Bases is owned by Agency

Data Center Consolidation Project Reporting Structure
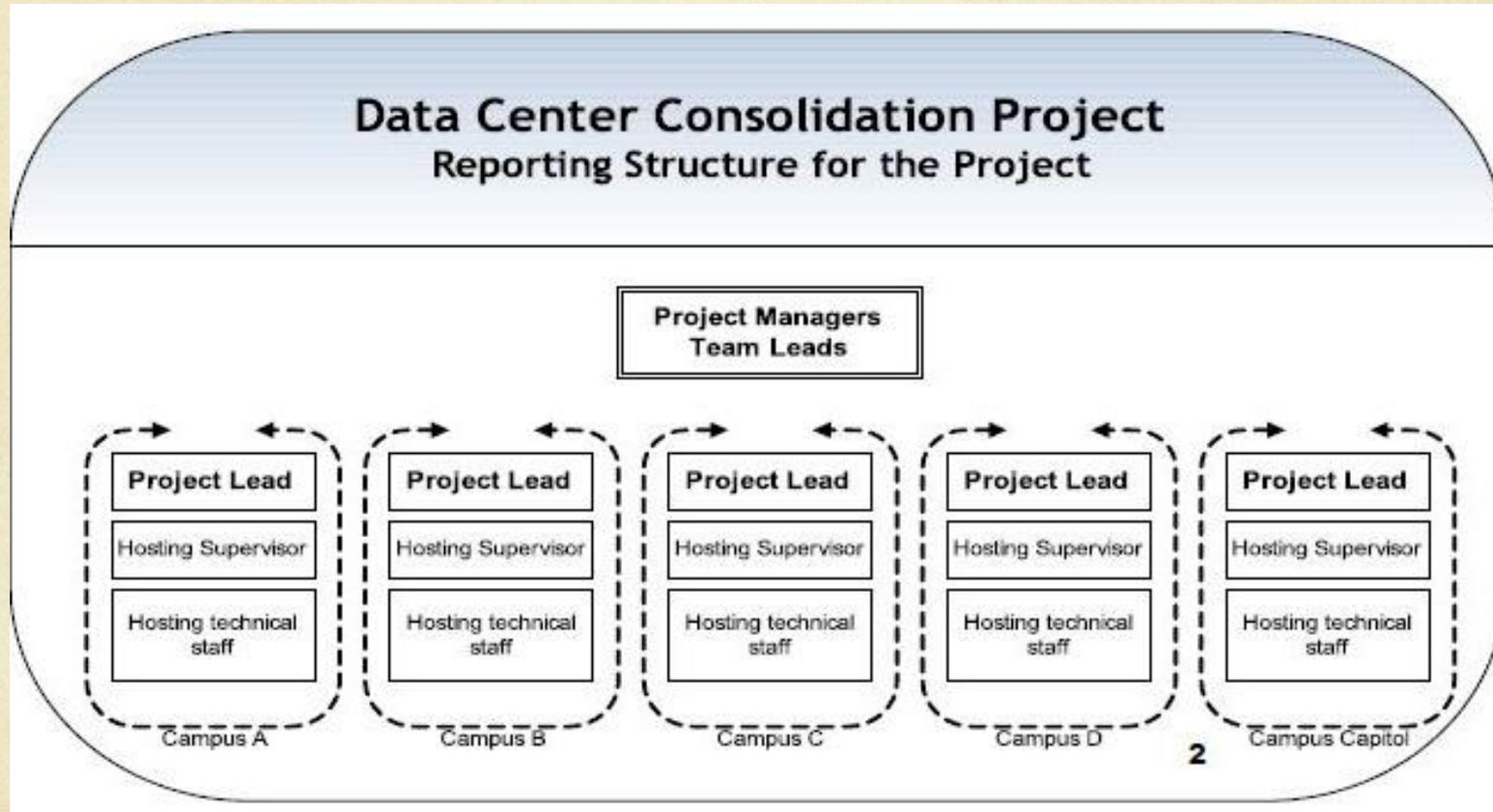
Ownership of Data Systems

- Discussions and agreements between parties up Front is critical

- State Data Center (State CIO)
  - What is the roll of the Enterprise (State Data Center)

  - Infrastructure of the Network
    - Firewalls
    - Connectivity - network
    - Security of the servers
    - Hosting
    - All infrastructure function

Ownership of Data Systems (cont.)

- Agency
  - Applications
  - All Data
  - Security of data
  - Training of Agency and DTS staff
  - Policy and procedures

Accomplishments

○ Successfully consolidated 35 existing data centers down to 2 data centers.

○ Successfully reduced physical server counts from 1864 servers, to 591 physical

○ servers, a 68% reduction in server counts.

○ Built out a scalable enterprise storage environment that allows for Tier 1, Tier 2,

○ and Tier 3 data storage

Lessons Learned Consolidation

- Support of executive management is essential to the success of the and provides a means to be accountable for reporting

- Ensure the project plan has clearly defined objectives and deliverables to prevent scope creep

- Give visibility to the progress of the project

- Regular communication is essential for a successful project

Lessons Learned (Cont.)

- Customer Communication - Maintain a high level of communication with the customer and the Campus IT manager about the project

- Not every campus can or should do their moves like the other campuses

- Set time frames for task completions to allow for application testing before/after server migrations

Security Of Tax Data

- October 2012 – State Department of Health had a data breach

- All of a sudden agencies deemed Security a high Priority

- Many agencies didn't have the requirement of a IRS 1075 to meet
  - One time I was grateful for the 1075

Remediation Taken

- Data classification in all systems state wide

- Risk Assessments (High, Medium, Low) by agency and with consultation form DTS

- Outside Consultant hired to a Statewide security assessment

- Statewide Security Council created

- Security Ownership Identified

Security Ownership

- Network, Hosting, and Infrastructure
  - Enterprise (Statewide DTS)
  - Blocks between 300 Milllion

- Application, Data, Policy and Procedure
  - Agency
  - Responsibility of audit
  - Accountability for security to the public is Agency

Email Security Google Mail

○ November 2001 State Dept. of Technology (DTS) notified all State agencies that Google Apps was selected as the replacement for Group Wise

○ Implementation planned for May 2012

○ January 2012 – Tax submitted their 45-day notice to the IRS letting them know of scheduled move to Google

○ February 2012 – Tax notified DTS and Google of four 1075 compliance requirements

Email Security (cont.)

- May 2012 – IRS Office of Safegards onsite visit to Google Data Center in Washington DC

- June 2012 – Tax worked with DTS to implement customer defined security controls

- June 2012 – Received approval from IRS

- November 2012 – All State of Utah employees migrated to Google Apps

Challenges

○ Getting DTS to understand the need to involve the IRS in the transition

○ Google assumed that since they were FISMA compliant, that also meant they were Pub. 1075 compliant.

○ Email servers are not considered remote, requiring 2-factor authentication to access email. Token cost were around $70.00 per person

○ Encryption and archiving of emails was not included in the original Google contract. Additional cost of $40.00 per person - **Extremely tight timeframe for completion**

Resolutions

○ Held numerous conference calls with the IRS Office of Safegards, Booz Allen Hamilton, DTS and Google

○ Internal meetings with project team; weekly meeting with core project team; sub-team met multiple times per week

○ Follow up, follow up, follow up

○ Training of all employees: online videos, Google guides, Instructor led training on encryption - labeling

Resolutions (cont.)

- Implement recommended controls:
  - Labeling
  - Encryption
  - Audit trails/Logging
  - retained for 10 years
  - 2-factor authentication
  - RSA SecurID tokens
  - Policy & procedure update

Where We Are Today

- Still tweaking procedures as we find better ways to do things

- Auditing process is extremely time consuming – need to compare multiple log files. Google is working on a solution to simplify the monitoring process

- Building test environment to allow testing of changes prior to the move to production